How Cisco Secure IDS Responds to the Nimda Virus

Document ID: 13871

Contents

Introduction

This document explains how Cisco Secure Intrusion Detection System (IDS) identifies and prevents web server compromise from attacks by the Nimda worm (also known as the Concept virus). The complex technical workings of the worm are beyond the scope of this bulletin and are well documented elsewhere. One of the best technical descriptions of the Nimda worm can be found in CERT® Advisory CA–2001–26 Nimda Worm ⬈ .

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

The Nimda worm is a hybrid worm and virus that is spreading aggressively on the Internet. To understand Nimda and the abilities of Cisco IDS to mitigate its spread, it is important to define these two terms:

- **Worm** refers to malicious code that spreads automatically, without human intervention.
- **Virus** refers to malicious code that spreads through some type of human intervention, such as when you open an e–mail, browse an infected website, or manually execute an infected file.

The Nimda worm is actually a hybrid that exhibits characteristics of both a worm and a virus. Nimda infects in multiple ways, most of which require human intervention. Cisco IDS Host Sensor blocks worm–like infection methods that spread through vulnerabilities in Microsoft s Internet Information Server (IIS). Cisco IDS does not block the virus–like, manual infection methods, such as when you open an e–mail attachment, browse an infected website, or manually execute an infected file.

Cisco IDS Host Sensor Protects Against Nimda

Cisco IDS Host Sensor prevents Directory Traversal attacks, which include those used by the Nimda worm. When the worm attempts to compromise a Cisco IDS–protected web server, the attack fails and the server is not compromised.

These Cisco IDS Host Sensor rules prevent the success of the Nimda worm:

- IIS Directory Traversal (four rules)
- IIS Directory Traversal and Code Execution (four rules)
- IIS Double Hex Encoding Directory Traversal (four rules)

Cisco IDS Host Sensor also defends against unauthorized changes to web content, so it does not allow the worm to alter web pages in order to spread itself to other servers.

Cisco IDS conforms with standard security best practices to protect web servers against Nimda. These best practices dictate not to read e–mail or browse the web from a production web server, as well as not have network shares open on a server. Cisco IDS Host Sensor prevents the web server from being compromised through HTTP and IIS exploits. The aforementioned best practices ensure that the Nimda worm does not arrive on the web server by some manual means.

Cisco IDS Network Sensor Identifies Nimda

Cisco IDS Network Sensor identifies web application attacks, which include those used by the Nimda worm. The Network Sensor is able to identify attacks and provide details about the affected or compromised hosts to isolate the Nimda infection.

These Cisco IDS Network Sensor alarms fire:

- WWW WinNT cmd.exe Access (SigID 5081)
- IIS CGI Double Decode (SigID 5124)
- WWW IIS Unicode Attack (SigID 5114)
- IIS Dot Dot Execute Attack (SigID 3215)
- IIS Dot Dot Crash Attack (SigID 3216)

Operators do not see an alarm that identifies Nimda by name. They see a series of the alarms noted as Nimda tries different exploits to compromise the target. The alarms identify the source address of hosts that have been compromised and that should be isolated from the network, cleaned, and patched.

Recommended Courses of Action

Follow these steps to protect against the Nimda worm:

1. Apply the latest updates for Microsoft Outlook, Outlook Express, Internet Explorer, and IIS available from Microsoft .
2. Update your virus–scanning software with the latest patch to mitigate the spread of the virus.

Note: You can download the latest virus patch to protect your PC from infection. If your PC has already been infected, this virus patch allows you to manually scan the hard drive of your PC and clean the infection from the machine.

3. Deploy Cisco IDS to mitigate the threat, contain the infection, and protect the servers.

Related Information

- **How to Protect Your Network Against the Nimda Virus**
- **Cisco Product Security Advisories and Notices**
- **Cisco Secure Intrusion Detection Support Page**
- **Documentation for Cisco Secure Intrusion Detection System**
- **Technical Support – Cisco Systems**

Updated: Jan 19, 2006   Document ID: 13871